WORMS A NOVA AMEAÇA

No dia 25 de janeiro de 2003, um sábado, o tráfego da Internet foi afetado por um worm cuja propagação foi a mais rápida já vista. Durante os três primeiros minutos enquanto o worm se espalhava, à cada 8,5 segundos o número de máquinas infectadas duplicava. Isto foi 250 vezes mais rápido que o Code Red, que na metade de 2001 duplicou-se à cada 37 minutos! Em 10 minutos do início do ataque cerca de 75.000 máquinas estavam infectadas.

Este worm é o SQL Slammer, de apenas 376 Bytes!

Os worms tem representado uma ameaça cada vez maior e tem sido já a bom tempo alvo da mídia, enquanto os vírus praticamente tem sido ignorados. Por que isso acontece?

Primeiramente devemos entender as origens do termo Worm, saber quais as diferenças entre eles e os vírus, como eles funcionam para compreender por que seu potencial destrutivo e infeccioso excede o dos vírus de computador.

AS ORIGENS

O termo "Worm" atual é derivado da história de ficção científica escrita por John Brunner em 1975, chamada "Shockwave Rider", na qual um governo totalitário controlava os cidadãos por meio de uma poderosa rede de computadores. Os que lutavam pela liberdade infestaram a rede com um programa chamado "Tapeworm", obrigando o governo desativar a rede, destruindo a base de seu poder.

Os primeiros Worms era programas pequenos e simples criados para favorecer um melhor uso de uma rede de computadores.

O primeiro programa que poderia receber esse nome foi escrito em 1971 por Bob Thomas. Esse programa era uma resposta às suas necessidades como controlador de tráfego aéreo e ajudava a notificar os operadores quando o controle de uma aeronave era movido de um computador para outro.

Em 1982 John Shock e Jon Hepps do centro de pesquisa da Xerox em Palo Alto começaram a fazer experimentos com programas do tipo Worm (foi a primeira vez em que o termo foi aplicado para este tipo de código). Eles criaram 5 worms, destinados a tarefas úteis em sua rede, porém um desses worms, o "Vampire" (cuja tarefa era ficar "adormecido" durante o dia mas, de noite, se ativava para aproveitar que a maioria dos computadores estava sendo subutilizada para processar tarefas complexas usando assim essa capacidade ociosa), teve falhas de operação causando travamento do sistema e impossibilitava sua reativação (travando cerca de 100 máquinas). Os pesquisadores tiveram então que desenvolver uma "vacina" para prevenir que o worm novamente causasse problema.

O vírus "Árvore de Natal", (Christmas Tree) surgido em dezembro de 1987 talvez tenha sido o primeiro "worm" a se propagar por rede, ele foi criado e manejado para paralizar os computadores IBM no dia de Natal de 1987, espalhando-se pela BITNET ("Because It's Time Network" - Uma rede que ligava mainframes IBM) .

Mas desde 1982 até 2 de novembro de 1988, os Worms ficaram fora do foco da mídia. Nessa data um worm criado por Robert Morris, um graduado em ciências da universidade de Cornell, "acidentalmente" foi lançado na Arpanet (precursora da atual Internet) espalhando-se em suas 8 horas de atividade por aproximadamente 6.000 máquinas, tendo se tornado machete e atraído a atenção a esse tipo de programa por ter causado prejuízos entre US$ 100.000,00 e US$ 10.000.000,00 segundo o United States General Accounting Office, e em 1989 o CERT (Computer Emergency Response Team) já alertava sobre o "Wank" (de "Worms against Nuclear Killers!"), um worm que aproveitava falhas de segurança e bugs para se espalhar pela rede "SPAN" infectando muitos computadores VAX e VMS e já levava uma "carga destrutiva" como: desativar o sistema de email, alterar senhas e deletar usuários registrados.

Desde então os worms tem se diversificado, tornando-se extremamente daninhos, capazes inclusive de portar outros worms e até vírus em seu interior, como o W32.Klez.gen@mm que pode portar o perigoso CIH, vulgo Chernobill, capaz de inutilizar por completo o HD.

MAS O QUE É UM WORM?

Um vírus é um programa de computador que infecta outro programa, copiando seu código para dele, geralmente o modificando de forma a que o código do vírus seja rodado inicialmente caso o programa seja executado. Um worm não faz isso, ele é um programa autônomo. Ele pode até alterar outros arquivos para atenderem às suas necessidades ou infiltrar versões alteradas de outros programas, mas por não se embutir, eles precisam instalar no sistema operacional meios através dos quais possam ser ativados. O Sircam, por exemplo, altera o registro do Windows para que toda vez que um programa (.exe) for executado ele seja ativado, o BugBear se instala na chave de inicialização do Windows.

COMO FUNCIONA UM WORM?

Um worm não surge do nada. Como qualquer programa de computador ele precisa "entrar" na máquina de alguma maneira. Alguns worms, como o Love Letter ou o Melissa, se espalham por meio de anexos de email, o Opaserv vasculha as redes em busca de máquinas que forneçam acesso por NetBios sem proteção ao compartilhamento, enfim, um worm pode se instalar ou infectar seu micro por meio de uma ação do usuário (worms codependentes) ou podem agir "na surdina" (worms solitários) de forma independente. A primeira coisa que um worm ao ser executado em uma máquina faz é verificar se a

máquina já está ou não infectada. Se não estiver ele efetua essa infecção e procura colocar um meio para ser ativado novamente quando o sistema for reiniciado.
Depois ele tenta infectar outros computadores, conforme foi programado, através de emails ou por meio de falhas nas redes ou nos micros que estejam on-line.

Vários worms usam rastreadores de IP (randômicos como o SQL Slammer, por exemplo, ou derivados de uma análise da rede local por máscara de subrede, como o Opaserv) de modo a enviar cópias de seu código e executá-las no computador alvo.

A maioria dos worms levam, além, uma "carga destrutiva", um conjunto de ações e rotinas que visam prejudicar o desempenho do computador, danificar ou corromper arquivos ou até mesmo o próprio sistema.

POR QUE SEU POTENCIAL DESTRUTIVO E INFECCIOSO É SUPERIOR AO DOS VÍRUS?

Um vírus de computador possui algumas limitações técnicas derivadas de sua natureza virótica. Um vírus não pode ter um tamanho excessivamente grande. Deve ser criado em hexadecimal, assembler, linguagem C ou qualquer outra que garanta maiores chances de execução. Já um worm, como programa independente, pode usar todos os recursos oferecidos pelo sistema, como scripting, funções API, pode buscar atualizações e pluggins, carregar vírus ou outros worms dentro de sí, vários desativam os mais famosos programas antivírus e firewalls (como o BugBear e o Klez) e não possui limites "teóricos" de suas ações, podendo fazer tudo que qualquer outro software faria, incluindo usar sniffers pra detecção de tráfego, keyloggers para pegar senhas de usuário, enviar emails sem necessidade de outros programas de email para isso e são muito mais fáceis de serem escritos que os vírus (o Worm Anna Kournikova, por exemplo, foi criado através de um Kit de criação de worms desenvolvido por um programador argentino).

Não existe sistema invulnerável e perfeito, mas os usuários e administradores de sistema são em grande parte responsáveis por suas vulnerabilidades. Normalmente as empresas dispõe patches de correção das falhas assim que elas são detectadas, mas ninguém se importa muito em fazer essas "correções", bem como é indispensável o uso de um bom antivírus que deve ser mantido atualizado, usar um firewall (sem o qual worms como o Opaserv tem grande possibilidade de infectar seu computador) e ferramentas auxiliares que possam parar os vírus caso eles parem o software antivírus (um bom software para essa finalidade é o nosso Alerta-Z).

Como diz o antigo adágio: “prevenção e canja de galinha não fazem mal a ninguém”!